PRODUCTS IN RESIDUE CLASSES

JOHN B. FRIEDLANDER, PÄR KURLBERG, AND IGOR E. SHPARLINSKI

Abstract. We consider a problem of P. Erdős, A. M. Odlyzko and A. Sárkőzy about the representation of residue classes modulo m by products of two not too large primes. While it seems that even the Extended Riemann Hypothesis is not powerful enough to achieve the expected results, here we obtain some unconditional results "on average" over moduli m and residue classes modulo m and somewhat stronger results when the average is restricted to prime moduli $m = p$. We also consider the analogous question wherein the primes are replaced by easier sequences so, quite naturally, we obtain much stronger results.

1. Introduction

Let m and a be integers with $m \geq 1$ and $\gcd(a, m) = 1$. For $\mathcal{R}$ and $\mathcal{S}$, sets of positive integers, we consider the question of whether there are integers $r \in \mathcal{R}$ and $s \in \mathcal{S}$ such that

$$rs \equiv a \pmod{m}$$

and, if so, how small can we choose these factors to be.

An obvious greedy algorithm would be to choose some small value for one of these, say r, and then look for the least $s \in \mathcal{S}$ which satisfies the congruence

$$s \equiv a\overline{r} \pmod{m}\ , \tag{1}$$

where $\overline{r}$ indicates the multiplicative inverse of r modulo m. It is clear that the use of this strategy usually limits the possibility for choosing s to a range $s \leq m^{1+o(1)}$. Hence, to even obtain a bound $r < m$, $s < m$ requires a more delicate argument and represents a result of a different order of difficulty. Actually, one could even hope to attain a bound

$$r,\ s \leq m^{\frac{1}{2}+o(1)}\ ,$$

a better result being hopeless, but such a goal seems far away even in the simplest case where $\mathcal{R} = \mathcal{S}$ is the set of all positive integers.

We are especially interested in the problem where $\mathcal{R} = \mathcal{S}$ is the set of primes. In this case we denote by $P(x; m, a)$ the number of solutions

to the congruence

$$p_1 p_2 \equiv a \pmod{m}$$

in primes $p_1, p_2 \le x$, and we are interested in studying $P(x; m, a)$ for values of x, as small as possible, for example for $x = m$.

Our work has been motivated by the study of the quantity $P(x; m, a)$ in the paper [3] of P. Erdős, A. M. Odlyzko and A. Sárkőzy. They prove a number of results conditional on various assumptions about the zero-free regions for Dirichlet L–functions. However, even the Extended Riemann Hypothesis[1] (ERH) seems not to be powerful enough to prove their intended goal that

$$P(m; m, a) > 0$$

whenever $\gcd(a, m) = 1$. Furthermore, even various relaxations of this question considered in [3] have required some unproven assumptions. In particular, under a certain weakened form of the ERH, the mean-square

$$P(x, m) = \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m} \left(P(x; m, a) - \frac{\pi(x)^2}{\varphi(m)} \right)^2$$

has been estimated successfully in the case $x = m$ and m prime. Here, as usual, $\varphi(k)$ is the Euler function and $\pi(x)$ is the number of primes $p \le x$

We further relax the original question but instead concentrate on unconditional results. In particular, in Section 2 we use the large sieve to estimate $P(x, q)$ on average over primes $M < q \le 2M$ in ranges $M \ge x$ and also $P(x, m)$ over general integer moduli m. In the case of the average over prime moduli we can come within a power of a logarithm of the optimal range.

We also study the problem for some integer sets a little less difficult than the primes. For example, the sequence of squarefree integers is one which can be handled with greater success and without any unproved assumptions. Let $S(x; m, a)$ denote the counterpart of $P(x; m, a)$ wherein the primes p_1, p_2 are replaced by squarefree integers. Here, in Section 3, we obtain an asymptotic formula for $S(x; m, a)$ which is nontrivial for $x \ge m^{3/4+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large m. As hinted above, one might hope that such formulas hold even down as far as $x \ge m^{1/2+\varepsilon}$ but if so this seems quite difficult. We do not know how to get a wider range of uniformity (apart from the ε) even for the apparently easier problem where we do not insist

[1]The assertion that all nontrivial zeros of any Dirichlet L-function lie on the critical line.

that the factors be squarefree! In this case, where $\mathcal{R} = \mathcal{S}$ is the set of all positive integers, the exponent 3/4 rests on the Weil bound for Kloosterman sums and has resisted improvement for half a century. See however [8, 15] for recent work related to this problem.

In Section 4 we consider the hybrid problem with products ps of a prime p and a squarefree integer s in the range $p, s \le m^{1/2+\varepsilon}$ and show that, for any integer m, these products represent almost all reduced residue classes modulo m the expected number of times.

Finally, in Section 5 we consider a different example wherein one of the two factor sets is a sumset, a case in which rather general results can be obtained provided neither set is very thin. We also consider the case of products of two primes and one shifted prime which is also accessible by present methods.

Throughout the paper the letters p and q are reserved for prime numbers. The Möbius function μ and divisor function τ have their usual meanings.

Acknowledgements. Much of the work on this paper was done during visits by P. K. and I. S. to the University of Toronto, whose support and hospitality are gratefully acknowledged. Research of J. F. was partially supported by NSERC grant A5123, that of P.K. by grants from the Göran Gustafsson Foundation, and the Royal Swedish Academy of Sciences, and that of I. S. by ARC grant DP0556431.

2. Products of Primes

We note that, for a sufficiently large constant c, the result of Heath-Brown [12] on the Linnik problem of the least prime in an arithmetic progression implies by (1) that $P(x; m, a) > 0$ for any a such that $\gcd(a, m) = 1$, provided $x \ge cm^{11/2}$, and it has long been known that, under the ERH, the exponent 11/2 may be replaced by any number larger than 2.

It is even expected that $x \ge m^{1+\varepsilon}$ for any fixed $\varepsilon > 0$ is admissible but ideas for any reasonable approach to this are lacking, at least for individual progressions. However, one can show, again using the greedy algorithm (1) but now in conjunction with the Barban-Davenport-Halberstam Theorem (see [13, Theorem 17.2]), that $P(x; m, a) > 0$ for most $m \le M$ and most reduced classes modulo m provided that $x/M(\log M)^3 \to \infty$. However, we are able to do better than that with a different argument.

Let us define

$$R(x,M)=\sum_{M<m\le 2M} P(x,m) \quad \text{and} \quad R_\pi(x,M)=\sum_{M<q\le 2M} P(x,q)\ ,$$

where, as usual, q runs over primes.

We now improve on the trivial bounds:

$$R(x,M)\ll x^4 \quad \text{and} \quad R_\pi(x,M)\ll x^4/\log x.$$

Theorem 1. *The following bounds hold:*

$$R(x,M)\ll x^4(\log x)^{-A}+Mx^2,$$

for any A, with an implied constant that depends on A, and

$$R_\pi(x,M)\ll \left(M^{-1}x^4+Mx^2\right)(\log x)^{-2}\ .$$

Proof. Let $\mathcal{X}_m$ be the set of all $\varphi(m)$ multiplicative characters modulo m, and $\mathcal{X}_m^*$ the set of primitive characters modulo m (which in the case of prime modulus q includes all such characters other than the principal character).

Using the orthogonality relation

$$\frac{1}{\varphi(m)}\sum_{\chi\in\mathcal{X}_m}\chi\left(r\right)=\begin{cases}1 & \text{if } r\equiv 1 \pmod m,\\ 0 & \text{otherwise,}\end{cases}$$

for $\gcd(a,m)=1$, we write

$$\begin{aligned}P(x;m,a) &= \sum_{p_1,p_2\le x}\frac{1}{\varphi(m)}\sum_{\chi\in\mathcal{X}_m}\chi\left(p_1p_2a^{-1}\right)\\ &= \frac{\pi(x)^2}{\varphi(m)}+\frac{1}{\varphi(m)}\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\ne\chi_0}}\chi\left(a^{-1}\right)\sum_{p_1,p_2\le x}\chi\left(p_1p_2\right)\\ &= \frac{\pi(x)^2}{\varphi(m)}+\frac{1}{\varphi(m)}\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\ne\chi_0}}\chi\left(a^{-1}\right)T_\chi(x)^2\end{aligned}$$

where

$$T_\chi(x)=\sum_{p\le x}\chi\left(p\right).$$

In particular,

$$\begin{aligned} P(x,m) &= \frac{1}{\varphi(m)^2}\sum_{(a,m)=1}\left(\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\neq\chi_0}}\chi\left(a^{-1}\right)\left(\sum_{p\le x}\chi\left(p\right)\right)^2\right)^2 \\ &\le \frac{1}{\varphi(m)^2}\sum_{(a,m)=1}\left|\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\neq\chi_0}}\overline{\chi}\left(a\right)T_\chi(x)^2\right|^2 \\ &= \frac{1}{\varphi(m)^2}\sum_{(a,m)=1}\sum_{\chi_1,\chi_2\neq\chi_0}\overline{\chi}_1\left(a\right)\chi_2\left(a\right)T_{\chi_1}(x)^2T_{\overline{\chi}_2}(x)^2 \\ &= \frac{1}{\varphi(m)^2}\sum_{\chi_1,\chi_2\neq\chi_0}T_{\chi_1}(x)^2T_{\overline{\chi}_2}(x)^2\sum_{(a,m)=1}\overline{\chi}_1\left(a\right)\chi_2\left(a\right)\ , \end{aligned}$$

where $\overline{\chi}$ denotes the conjugate character. Since

$$\sum_{(a,m)=1}\overline{\chi}_1\left(a\right)\chi_2\left(a\right)=\begin{cases}\varphi(m) & \text{if } \chi_1=\chi_2,\\ 0 & \text{otherwise,}\end{cases}$$

we obtain

$$P(x,m)\le\frac{1}{\varphi(m)}\sum_{\chi\neq\chi_0}T_\chi(x)^2T_{\overline{\chi}}(x)^2=\frac{1}{\varphi(m)}\sum_{\chi\neq\chi_0}\left|T_\chi(x)\right|^4.$$

We remark that

$$T_\chi(x)^2=\sum_{n\le x^2}a_n\chi(n)$$

where $a_n=2$ if $n=p_1p_2$ for two distinct primes $p_1,p_2\le x$, $a_n=1$ if n is the square of a prime $p\le x$, and $a_n=0$ otherwise. Hence

$$P(x,m)\le\frac{1}{\varphi(m)}\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\neq\chi_0}}\left|\sum_{n\le x^2}a_n\chi(n)\right|^2$$

which leads to the bound

$$\sum_{M<m\le 2M}P(x,m)\le\sum_{M<m\le 2M}\frac{1}{\varphi(m)}\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\neq\chi_0}}\left|\sum_{n\le x^2}a_n\chi(n)\right|^2. \tag{2}$$

We first treat the simpler case where the average is over prime moduli $m=q$ so that all non-principal characters modulo q are primitive and (2) can be replaced by the bound

$$\sum_{M<q\le 2M}P(x,q)\ll\frac{1}{M}\sum_{M<q\le 2M}\sum_{\chi\in\mathcal{X}_q^*}\left|\sum_{n\le x^2}a_n\chi(n)\right|^2.$$

By the multiplicative form of the large sieve inequality, see for example [13, Theorem 7.13], we have

$$\begin{aligned}\sum_{M<q\le 2M}\sum_{\chi\in\mathcal{X}_q^*}\Big|\sum_{n\le x^2}a_n\chi(n)\Big|^2 &\ll (M^2+x^2)\sum_{n\le x^2}a_n^2\\ &\ll (M^2+x^2)x^2(\log x)^{-2}\ .\end{aligned}$$

Therefore,

$$R_\pi(x,M)=\sum_{M<q\le 2M}P(x,q)\ll (Mx^2+M^{-1}x^4)(\log x)^{-2}\ ,$$

which concludes the proof for the case of prime moduli.

We now turn to the case of general modulus m and need to estimate, this time in general, the sum

$$S=\sum_{M<m\le 2M}\frac{1}{\varphi(m)}\sum_{\substack{\chi\in\mathcal{X}_m\\ \chi\ne\chi_0}}\Big|\sum_{n\le x^2}a_n\chi(n)\Big|^2$$

on the right hand side of inequality (2). Given a character χ modulo m occurring in this sum, let χ be induced by a primitive character ψ modulo f where $m=fe$ and, since χ is non-principal, $f>1$. We have

$$\sum_{n\le x^2}a_n\chi(n)=\sum_{\substack{n\le x^2\\ \gcd(n,e)=1}}a_n\psi(n)=\sum_{n\le x^2}a_n\psi(n)+O(\log^2 e)$$

in view of the definition of a_n. Using this and the inequality $\varphi(fe)\ge\varphi(f)\varphi(e)$, we have

$$\begin{aligned}S&\le\sum_{e\le 2M}\frac{1}{\varphi(e)}\sum_{2\le f\le 2M/e}\frac{1}{\varphi(f)}\sum_{\psi\in\mathcal{X}_f^*}\Big|\sum_{n\le x^2}a_n\psi(n)\Big|^2+O(Mx^2)\\ &=\sum_{e\le 2M}\frac{1}{\varphi(e)}\{S_e(f\le F)+S_e(f>F)\}+O(Mx^2)\ ,\end{aligned}$$

say, where $F=(\log x)^B$ for some large fixed B and $S_e(f\le F)$ and $S_e(f>F)$ are the parts of the inner sums taken over $f\le F$ and $f>F$, respectively. (Note that we can assume $\log M\ll\log x$ else the theorem is trivial.) For $2\le f\le F$ we split the sum over n into arithmetic progressions modulo f and apply to each of them the bound

$$\sum_{\substack{n\le x^2\\ n\equiv b\pmod f}}a_n-\frac{1}{\varphi(f)}\sum_{\substack{n\le x^2\\ \gcd(n,f)=1}}a_n\ll x^2(\log x)^{-C}$$

for any C, which follows quickly from the Siegel-Walfisz theorem. Using orthogonality the main term in the sum over n disappears and we obtain for each ψ the bound

$$\sum_{n\le x^2} a_n\psi(n) \ll Fx^2(\log x)^{-C}$$

from which we derive

$$S_e(f \le F) \ll F^3x^4(\log x)^{-2C} \ .$$

For the sum over $f > F$ we split the sum into $\ll \log 2M$ dyadic intervals $(V, 2V]$ and apply again the same large sieve inequality as we did in the case of prime moduli. We obtain

$$\begin{aligned} S_e(f > F) &\ll \log 2M \sup_{F\le V\le 2M} V^{-1}(V^2 + x^2) \sum_{n\le x^2} |a_n|^2 \\ &\ll (M + F^{-1}x^2)x^2 \ll Mx^2 + x^4(\log x)^{-B} \ . \end{aligned}$$

We take $C = 2B,\ B = A+1$, and sum over e, completing the proof. □

We remark that the Siegel-Walfisz theorem restricts us to choose F no larger than a fixed power of $\log x$ which limits the saving in Theorem 1 in this case of general modulus.

Let $W(M, x)$ be the number of pairs (q, a) where the prime q and integer a satisfy $M < q \le 2M$ and $1 \le a < q$ and such that $P(x; q, a) = 0$. Then

$$\frac{\pi(x)^4}{4M^2} W(M, x) \le R_\pi(x, M).$$

Hence by Theorem 1 we have

$$W(M, x) = o(M\pi(M))$$

for any $x \le M$ satisfying $xM^{-1/2}(\log M)^{-3/2} \to \infty$, which is thus within a power of the logarithm of being best possible. This may be compared with a result of M. Z. Garaev [7] wherein a better power of the logarithm is obtained, but for products of integers, not necessarily prime.

Finally, taking $x = M$ we see that,

$$W(M, M) \ll M(\log M)^2.$$

3. Products of Squarefree Integers

As in the case of products of primes we can quickly deduce some bound by appealing to the known results, in this case for the smallest square-free integer in an arithmetic progression. Thus, from the result of Heath-Brown [11] on that problem it follows trivially that

$S(x; m, a) > 0$ for any a such that $\gcd(a, m)$ is square-free, provided $x \geq m^{13/9+\varepsilon}$.

Theorem 2. *For all integers $m \geq 1$ and a with $\gcd(a, m) = 1$ and real positive x, we have*

$$S(x; m, a) = \frac{36}{\pi^4} \cdot \frac{x^2}{m} \prod_{p \mid m} \left(1 + \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^3}\right)^{-1} + O\left(xm^{-1/4+o(1)}\right),$$

where the product is taken over all prime numbers $p \mid m$.

We remark that, as stated in the introduction, this gives the asymptotic formula in the range $x \geq m^{3/4+\varepsilon}$ for fixed positive ε. We take $x < m$ in the proof. A very slight modification is needed for larger x.

Proof. For real U and V we demote by $N(U, V; m, b)$ the number of solutions to the congruence $uv \equiv b \pmod m$ in positive integers $u \leq U$, $v \leq V$.

Recall that $\mu(d)$ denotes the Möbius function. By the inclusion-exclusion principle, we write

$$S(x; m, a) = \sum_{\substack{d,e=1 \\ \gcd(de,m)=1}}^{\infty} \mu(d)\mu(e) N(x/d^2, x/e^2; m, ad^{-2}e^{-2}). \tag{3}$$

A standard application of bounds for incomplete Kloosterman sums (see [13, Corollary 11.12]) leads to the asymptotic formula

$$N(U, V; m, b) = UV\frac{\varphi(m)}{m^2} + O(m^{1/2+o(1)}) \tag{4}$$

uniformly over integers b with $\gcd(b, m) = 1$, see [1, 6] and references therein.

For $\tau(w)$, the number of positive divisors of w, we recall the well known bound

$$\tau(w) = w^{o(1)}, \tag{5}$$

see for example [19, Section I.5.2].

We define two quantities

$$y = xm^{-3/4} \qquad \text{and} \qquad z = xm^{-1/2}\ , \tag{6}$$

which will feature in the proof.

We use the asymptotic formula (4) for $de \le y$. which after substitution in (3) yields

$$S(x;m,a) = x^2\frac{\varphi(m)}{m^2} \sum_{\substack{de\le y\\ \gcd(de,m)=1}} \frac{\mu(d)\mu(e)}{d^2e^2} + O\left(ym^{1/2+o(1)} + \sum_{\substack{de>y\\ \gcd(de,m)=1}} N(x/d^2, x/e^2; m, ad^{-2}e^{-2})\right)$$

(since by (5) there are at most $y^{1+o(1)} = ym^{o(1)}$ such pairs (d,e) in the first sum).

Using (5), for the first term we obtain

$$\begin{aligned}\sum_{\substack{de\le y\\ \gcd(de,m)=1}} \frac{\mu(d)\mu(e)}{d^2e^2} &= \sum_{\substack{d,e=1\\ \gcd(de,m)=1}}^{\infty} \frac{\mu(d)\mu(e)}{d^2e^2} + O\left(\sum_{k\ge y}\frac{\tau(k)}{k^2}\right)\\ &= \left(\sum_{\substack{d=1\\ \gcd(d,m)=1}}^{\infty} \frac{\mu(d)}{d^2}\right)^2 + O(y^{-1+o(1)}).\end{aligned}$$

We have

$$\sum_{\substack{d=1\\ \gcd(d,m)=1}}^{\infty} \frac{\mu(d)}{d^2} = \prod_{p\nmid m}\left(1-\frac{1}{p^2}\right) = \zeta(2)\prod_{p\mid m}\left(1-\frac{1}{p^2}\right)^{-1},$$

where $\zeta(s)$ is the Riemann zeta-function. Therefore

$$\begin{aligned}S(x;m,a) = \frac{36}{\pi^4}x^2\frac{\varphi(m)}{m^2}\prod_{p\mid m}\left(1-\frac{1}{p^2}\right)^{-1}\\ + O\left(ym^{1/2+o(1)} + x^2y^{-1}m^{-1+o(1)} + \sum_{j=0}^{J}\Delta_j\right),\end{aligned} \tag{7}$$

where

$$J = \lceil 2\log(x/z)\rceil$$

and

$$\begin{aligned}\Delta_0 &= \sum_{\substack{z\ge de>y\\ \gcd(de,m)=1}} N(x/d^2, x/e^2; m, ad^{-2}e^{-2}),\\ \Delta_j &= \sum_{\substack{2^j z\ge de>2^{j-1}z\\ \gcd(de,m)=1}} N(x/d^2, x/e^2; m, ad^{-2}e^{-2}), \quad j=1,\dots J.\end{aligned}$$

To estimate Δ_0, we note that if $uv \equiv ad^{-2}e^{-2} \pmod m$ and with $1 \le u \le x/d^2$ and $1 \le v \le x/e^2$ then for each fixed pair (d,e), the product $w = uv \le x^2d^{-2}e^{-2}$ belongs to a prescribed residue class modulo m and thus takes at most $x^2d^{-2}e^{-2}m^{-1}+1$ possible values. In turn, each value of w gives rise to $\tau(w) = w^{o(1)} = m^{o(1)}$ pairs (u,v) with $uv = w$, see (5). Therefore

$$\begin{aligned}\Delta_0 &\le \sum_{\substack{z\ge de>y\\ \gcd(de,m)=1}} \left(\frac{x^2}{d^2e^2m}+1\right) m^{o(1)} = x^2m^{-1+o(1)} \sum_{de\ge y} \frac{1}{d^2e^2} + zm^{o(1)}\\ &= x^2m^{-1+o(1)} \sum_{k\ge y} \frac{\tau(k)}{k^2} + zm^{o(1)} = x^2y^{-1}m^{-1+o(1)} + zm^{o(1)}.\end{aligned}$$

To estimate Δ_j, with $j \ge 1$, we note that Δ_j does not exceed the number of pairs (d,e) of positive integers such that $de \le 2^j z$, $\gcd(de,m) = 1$ and $ad^{-2}e^{-2} \equiv w \pmod m$ for some positive integer $w \le W_j$ where

$$W_j = 4\frac{x^2}{2^{2j}z^2}, \qquad j = 1,\dots J.$$

Furthermore, due to our choice of z, see (6), we have $W_j \le m$. Thus if d and e are fixed, then solutions to the congruence $uv \equiv ad^{-2}e^{-2} \equiv w \pmod m$, where $1 \le w < m$, in positive integers $u \le x/d^2$, $v \le x/e^2$ satisfy the equation $uv = w$. Hence, by (5), every pair d and e leads to $\tau(w) = m^{o(1)}$ possible pairs (u,v). Collecting together d and e with the same value of $de = k$, and using (5) again,

$$\Delta_j \le m^{o(1)} T(2^j z, W_j), \qquad j = 1,\dots,J,$$

where $T(K,W)$ is the number of positive integers $k \le K$, $\gcd(k,m) = 1$ and $ak^{-2} \equiv w \pmod m$ for some positive integer $w \le W$.

Using exactly the same arguments as, for example in [17, Lemma 1] (Fourier expansion of the remainder term in the counting function, completion of the relevant exponential sum, and finally application of

Weil's theorem to the completed sum), we obtain that if $W < m$ then

$$T(K,W) = \frac{W}{m} \sum_{\substack{k=1\\ \gcd(k,m)=1}}^{K} 1 + O\left(m^{1/2+o(1)}\right) \le \frac{KW}{m} + O\left(m^{1/2+o(1)}\right),$$

which in turn implies that

$$\Delta_j \le m^{o(1)} \left(\frac{x^2}{2^j z m} + m^{1/2}\right), \qquad j = 1, \ldots, J.$$

Therefore

$$\begin{aligned} \sum_{j=1}^{J} \Delta_j &\le x^2 z^{-1} m^{-1+o(1)} \sum_{j=1}^{J} \frac{1}{2^j} + J m^{1/2+o(1)} \\ &\le x^2 z^{-1} m^{-1+o(1)} + m^{1/2+o(1)}. \end{aligned}$$

Substituting the bounds on Δ_0 and on Δ_j, $j = 1, \ldots, J$, in (7) we obtain

$$\begin{aligned} S(x;m,a) = \frac{36}{\pi^4} x^2 \frac{\varphi(m)}{m^2} \prod_{p \mid m} \left(1 - \frac{1}{p^2}\right)^{-1} \\ + O\left(y m^{1/2+o(1)} + x^2 y^{-1} m^{-1+o(1)} + z m^{o(1)}\right). \end{aligned}$$

Recalling the choice (6) of y and z, we conclude the proof. □

4. Products of Primes and Squarefree Integers

Here we study congruences $ps \equiv a \pmod m$ in primes $p \le x$ and squarefree integers $s \le x$.

In fact our approach works for congruences $rs \equiv a \pmod m$ where $r \le x$ is an element of a very general set $\mathcal{R}$ with $\gcd(r,m) = 1$ and $s \le x$ is squarefree. Accordingly, we write $Q(\mathcal{R}, x; m, a)$ for the number of solutions of such a congruence.

Theorem 3. *For all positive integers m, real x and sets $\mathcal{R} \subseteq [1,x]$ of integers r with $\gcd(r,m) = 1$, we have*

$$\sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} \left| Q(\mathcal{R}, x; m, a) - \vartheta_m \frac{|\mathcal{R}| x}{m} \right| \le |\mathcal{R}|^{3/4} x^{3/4} m^{1/4+o(1)},$$

where

$$\vartheta_m = \frac{6}{\pi^2} \prod_{p \mid m} \left(1 - \frac{1}{p^2}\right)^{-1}.$$

Proof. Since

$$\sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} Q(\mathcal{R}, x; m, a) \le |\mathcal{R}|x \ ,$$

we see that unless

$$|\mathcal{R}|x > m \tag{8}$$

the bound is trivial.

Let $U(\mathcal{R}, y; m, a)$ be the number of solutions to the congruence $ru \equiv a \pmod m$ in $r \in \mathcal{R}$ and positive integers $u \le y$. Our main tool is the bound

$$\sum_{a=1}^{m} \left| U(\mathcal{R}, y; m, a) - \frac{|\mathcal{R}|y}{m} \right|^2 \le |\mathcal{R}|xm^{o(1)}, \tag{9}$$

for $y \le x$, which has been given in [18].

For every positive integer $d \le x^{1/2}$ we denote by $V_d(\mathcal{R}, x; m, a)$ the number of solutions to the congruence $rv \equiv a \pmod m$ in $r \in R$ and positive integers $v \le x$ with $v \equiv 0 \pmod{d^2}$.

Using the inclusion-exclusion principle, we write

$$Q(\mathcal{R}, x; m, a) = \sum_{d=1}^{\infty} \mu(d) V_d(\mathcal{R}, x; m, a), \tag{10}$$

where, as before, $\mu(d)$ is the Möbius function.

Clearly, if $\gcd(a, m) = 1$ but $\gcd(d, m) > 1$, then $V_d(\mathcal{R}, x; m, a) = 0$. Furthermore, for $\gcd(ad, m) = 1$ we have

$$V_d(\mathcal{R}, x; m, a) = U(\mathcal{R}, x_d; m, a_d),$$

where $x_d = \lfloor x/d^2 \rfloor$ and a_d is defined by the congruence $a_d d^2 \equiv a \pmod m$, $1 \le a_d < m$.

We now choose some parameter $z \geq 1$, to be specified later and write (10)

$$\begin{aligned} Q(\mathcal{R}, x; m, a) &= \sum_{\substack{d=1 \\ \gcd(d,m)=1}}^{\infty} \mu(d) U(\mathcal{R}, x_d; m, a_d) \\ &= \sum_{\substack{d \leq z \\ \gcd(d,m)=1}} \mu(d) U(\mathcal{R}, x_d; m, a_d) \\ &\qquad + O\left(\sum_{x^{1/2} \geq d > z} U(\mathcal{R}, x_d; m, a_d) \right) \\ &= \sum_{\substack{d \leq z \\ \gcd(d,m)=1}} \mu(d) \frac{|\mathcal{R}| x_d}{m} + O\left(\sigma_1(a) + \sigma_2(a)\right), \end{aligned}$$

where

$$\begin{aligned} \sigma_1(a) &= \sum_{\substack{d \leq z \\ \gcd(d,m)=1}} \left| U(\mathcal{R}, x_d; m, a_d) - \frac{|\mathcal{R}| x_d}{m} \right| \\ \sigma_2(a) &= \sum_{\substack{x^{1/2} \geq d > z \\ \gcd(d,m)=1}} U(\mathcal{R}, x_d; m, a_d). \end{aligned}$$

As in the proof of Theorem 2, for the main term we obtain

$$\begin{aligned} \sum_{\substack{d \leq z \\ \gcd(d,m)=1}} \mu(d) \frac{|\mathcal{R}| x_d}{m} &= \frac{|\mathcal{R}| x}{m} \sum_{\substack{d \leq z \\ \gcd(d,m)=1}} \mu(d) \frac{1}{d^2} + O\left(\frac{z|\mathcal{R}|}{m} \right) \\ &= \vartheta_m \frac{|\mathcal{R}| x}{m} + O\left(\frac{|\mathcal{R}| x}{zm} + \frac{z|\mathcal{R}|}{m} \right). \end{aligned}$$

Accordingly we obtain

$$\sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m} \left| Q(\mathcal{R}, x; m, a) - \vartheta_m \frac{|\mathcal{R}| x}{m} \right| \ll \frac{|\mathcal{R}| x}{z} + z|\mathcal{R}| + \Sigma_1 + \Sigma_2, \tag{11}$$

where

$$\Sigma_1 = \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m} \sigma_1(a) \qquad \text{and} \qquad \Sigma_2 = \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m} \sigma_2(a).$$

Changing the order of summation and noticing that due to the condition $\gcd(d, m) = 1$, as a runs through all the reduced residue classes

modulo m then so does a_d, we write

$$\Sigma_1 = \sum_{\substack{d\le z\\ \gcd(d,m)=1}} \sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} \left| U(\mathcal{R}, x_d; m, a) - \frac{|\mathcal{R}|x_d}{m} \right|,$$

$$\Sigma_2 = \sum_{\substack{x^{1/2}\ge d>z\\ \gcd(d,m)=1}} \sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} U(\mathcal{R}, x_d; m, a).$$

By the Cauchy inequality and the bound (9), we have

$$\Sigma_1 \le \sum_{\substack{d\le z\\ \gcd(d,m)=1}} |\mathcal{R}|^{1/2} x^{1/2} m^{1/2+o(1)} \le z|\mathcal{R}|^{1/2} x^{1/2} m^{1/2+o(1)}. \tag{12}$$

Furthermore, it is clear that

$$\sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} U(\mathcal{R}, x_d; m, a) \le |\mathcal{R}|x_d \le |\mathcal{R}|x/d^2.$$

Therefore

$$\Sigma_2 \ll |\mathcal{R}|x \sum_{\substack{x^{1/2}\ge d>z\\ \gcd(d,m)=1}} \frac{1}{d^2} \ll \frac{|\mathcal{R}|x}{z}. \tag{13}$$

Substituting the bounds (12) and (13) in (11), we derive

$$\sum_{\substack{a=1\\ \gcd(a,m)=1}}^{m} \left| Q(\mathcal{R}, x; m, a) - \vartheta_m \frac{|\mathcal{R}|x}{m} \right| \ll \frac{|\mathcal{R}|x}{z} + z|\mathcal{R}| + z|\mathcal{R}|^{1/2} x^{1/2} m^{1/2+o(1)}.$$

Clearly $z|\mathcal{R}| \le z|\mathcal{R}|^{1/2}x^{1/2}m^{1/2}$, thus the second term in the last inequality can be dropped. Now taking $z = |\mathcal{R}|^{1/4}x^{1/4}m^{-1/4}$ and remarking that (8) implies that $z > 1$, we conclude the proof. □

We see that each reduced residue class modulo m which contains no integer of the form rs with $r \in \mathcal{R}$ and a squarefree integer $s \le x$ contributes a term of order $|\mathcal{R}|x/m$ to the sum estimated in Theorem 3.

If we take $x = m^{1/2+\varepsilon}$ for some fixed ε and $\mathcal{R}$ to be the set of primes $p \le x$ with $p \nmid m$, we see that the number of reduced classes modulo m which are not of the form ps with a prime $p \le x$ and a squarefree

integer $s \le x$, is at most

$$\begin{aligned} |\mathcal{R}|^{3/4}x^{3/4}m^{1/4+o(1)}m(|\mathcal{R}|x)^{-1} &\le |\mathcal{R}|^{-1/4}x^{-1/4}m^{5/4+o(1)} \\ &\le m^{1-\varepsilon/2+o(1)} \le m^{1-\varepsilon/3}, \end{aligned}$$

provided that m is large enough.

5. Some Other Products

Our work in this section is motivated by another nice, albeit conditional, result in [3], wherein it has been shown that if $\varepsilon > 0$ and q is large enough, then all invertible elements modulo q can be written as a product of three primes $p_1, p_2, p_3 < q$ under the assumption that all Dirichlet L-series $L(s,\chi)$ are non-vanishing for $\mathrm{Re}(s) > 1-(3+\varepsilon)\log\log q/\log q$ and $|\mathrm{Im}(s)| \le q$, for all non-trivial characters χ modulo q.

If we alter the problem slightly and consider numbers that are products of a prime and a sum of two primes, that is numbers of the form $p_1(p_2+p_3)$, we can unconditionally show that it suffices to take $p_1, p_2, p_3 < q^{1-\delta}$ for some $\delta > 0$ to obtain all residues modulo q. We also consider another modification, namely the representation of residue classes by the product $p_1p_2(p_3+b)$ of two primes and a shifted prime.

Theorem 4. *Let q be a prime. Given any invertible element a in $\mathbb{Z}/q\mathbb{Z}$, there are $\pi(X)^3/q + O(q^{3/16+o(1)}X^{57/32})$ primes $p_1, p_2, p_3 \le X < q$ such that $p_1(p_2+p_3) \equiv a \pmod q$.*

Proof. We have

$$\begin{aligned} &|\{p_1,p_2,p_3 \le X \ : \ p_1(p_2+p_3) \equiv a \pmod q\}| \\ &\qquad = \frac{1}{q}\sum_{t=1}^{q}\sum_{p_1,p_2,p_3\le X}\mathbf{e}_q(t(p_2+p_3-a\overline{p}_1)) \\ &\qquad = \frac{\pi(X)^3}{q} + \frac{1}{q}\sum_{t=1}^{q-1}\sum_{p_1\le X}\mathbf{e}_q(-ta\overline{p}_1)\sum_{p_2,p_3\le X}\mathbf{e}_q(t(p_2+p_3)). \end{aligned}$$

The error term is bounded by

$$\begin{aligned} &\frac{1}{q}\max_{t\not\equiv 0 \pmod q}\left|\sum_{p_1\le X}\mathbf{e}_q(-ta\overline{p}_1)\right|\cdot\sum_{t=1}^{q-1}\left|\sum_{p_2,p_3\le X}\mathbf{e}_q(t(p_2+p_3))\right| \\ &\qquad = \frac{1}{q}\max_{t\not\equiv 0 \pmod q}\left|\sum_{p_1\le X}\mathbf{e}_q(t\overline{p}_1)\right|\cdot\sum_{t=1}^{q-1}\left|\sum_{p_2\le X}\mathbf{e}_q(tp_2)\right|^2. \end{aligned}$$

By [4, Theorem 1.1] we have

$$\max_{t\not\equiv 0 \pmod q} \left| \sum_{p_1 \le X} \mathbf{e}_q(t\overline{p}_1) \right| \le q^{3/16+o(1)} X^{25/32}. \tag{14}$$

Also, by orthogonality we get

$$\sum_{t=1}^{q-1} \left| \sum_{p_2 \le X} \mathbf{e}_q(tp_2) \right|^2 = q\pi(X)$$

which concludes the proof. □

Clearly the asymptotic formula of Theorem 4 is nontrivial if $X \ge q^{38/39+\delta}$ for an arbitrary $\delta > 0$ and sufficiently large q.

We remark that the the proof of Theorem 4 extends immediately to yield the following more general result.

Theorem 5. *Let q be prime and $(a,q)=1$. Let $\mathcal{R}$ be any set of positive integers r with $(r,q)=1$ and $\mathcal{S}$ any set of integers $1 \le s < q$. Then we have*

$$\left| \sum_{\substack{r\in\mathcal{R}} } \sum_{s_1,s_2\in\mathcal{S}} \sum_{\substack{ \\ r(s_1+s_2)\equiv a \,(\bmod q)}} 1 - \frac{1}{q}|\mathcal{R}||\mathcal{S}|^2 \right| \le |\mathcal{S}| \max_{h\not\equiv 0 \,(\bmod q)} \left| \sum_{r\in\mathcal{R}} \mathbf{e}_q(h\overline{r}) \right| .$$

For example, in the case that $\mathcal{R}$ is the set of primes, then $\mathcal{S}$ can be replaced by an arbitrary set of residue classes modulo q satisfying $|\mathcal{S}| \ge q^{1-\delta}$ for some δ determined by the results of [2] or [4].

We now recall the bound of A. A. Karatsuba [14] which asserts that if q is prime and $X \ge q^{1/2+\varepsilon}$ for some ε, then for any fixed integer b with $\gcd(b,q)=1$,

$$\max_{\chi\in\mathcal{X}_q^*} \left| \sum_{p\le X} \chi(p+b) \right| \ll X^{1-\delta}, \tag{15}$$

where, as before, $\mathcal{X}_q^*$ is the set of all nontrivial multiplicative characters modulo q and $\delta > 0$ depends only on ε.

Using this bound in the the same way as in [5], one easily gets the following result:

Theorem 6. *Let q be a prime and let b be an integer with $\gcd(b,q)=1$. There are two absolute constants $\eta, \kappa > 0$ such that for $q > X \ge q^{1-\eta}$, for any invertible element a in $\mathbb{Z}/q\mathbb{Z}$, there are $(1+O(q^{-\kappa}))\pi(X)^3/q$ primes $p_1, p_2, p_3 \le X < q$ such that $p_1p_2(p_3+b) \equiv a \pmod q$.*

6. Remarks

We note that [2, Theorem A.9] and [4, Corollarie 1.6] give nontrivial estimates for the exponential sums in (14) as long as $X > q^{1/2+\varepsilon}$ and $X > q^{3/4+\varepsilon}$, respectively. However these bounds are less explicit than (14) and thus only lead to a weaker inexplicit statement.

In principle, Theorem 6 can be extended to composite moduli m and more general products. In fact, Z. Kh. Rakhmonov [16] provides an analogue of the bound (15), however only for $X \geq m^{1+\varepsilon}$.

We have already remarked on the work of M. Z. Garaev [7] showing that, in the case that $\mathcal{R} = \mathcal{S}$ is the set of all integers, one can come within a small power of the logarithm of the expected conjecture for most residue classes to most prime moduli. In very recent work, M. Z. Garaev and A. A. Karatsuba [10] have proved that in fact this holds for *all* prime moduli (see [9, 18] for various refinements of this result). Our bound for $R_\pi(x, M)$ in Theorem 1 gives in particular an analogue of the original result [7] in the apparently harder case when $\mathcal{R} = \mathcal{S}$ is the set of primes. However, obtaining an analogue to the result of [10] for the case of prime products remains an open problem.

References

[1] J. Beck and M. R. Khan, 'On the uniform distribution of inverses modulo n', *Period. Math. Hung.*, **44** (2002), 147–155.

[2] J. Bourgain, 'More on the sum-product phenomenon in prime fields and its applications', *Int. J. Number Theory*, **1** (2005), 1–32.

[3] P. Erdős, A. M. Odlyzko and A. Sárkőzy, 'On the residues of products of prime numbers', *Period. Math. Hung.*, **18** (1987), 229–239.

[4] E. Fouvry and P. Michel, 'Sur certaines sommes d'exponentielles sur les nombres premiers', *Ann. Sci. École Norm. Sup.*, **31** (1998), 93–130.

[5] J. B. Friedlander and I. E. Shparlinski, 'Least totient in a residue class', *Bull. Lond. Math. Soc.*, **39** (2007), 425–432.

[6] A. Fujii and Y. Kitaoka, 'On plain lattice points whose coordinates are reciprocals modulo a prime', *Nagoya Math. J.*, **147** (1997), 137–146.

[7] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a large prime', *Monatsh. Math.* , **148** (2006), 137–146.

[8] M. Z. Garaev, 'On the logarithmic factor in error term estimates in certain additive congruence problems', *Acta Arith.*, **124** (2006), 27–39.

[9] M. Z. Garaev and V. Garcia, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications', *Preprint*, 2007.

[10] M. Z. Garaev and A. A. Karatsuba, 'The representation of residue classes by products of small integers', *Proc. Edinburgh Math. Soc.*, **50** (2007), 363–375.

[11] D. R. Heath-Brown, 'The least square-free number in an arithmetic progression', *J. Reine Angew. Math.*, **332** (1982), 204–220.

[12] D. R. Heath-Brown, 'Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression', *Proc. London Math. Soc.* 64 (1992) 265–338.
[13] H. Iwaniec and E. Kowalski, *Analytic Number Theory* Amer. Math. Soc., Providence RI, 2004.
[14] A. A. Karatsuba, 'Sums of characters with prime numbers', *Izv. Akad. Nauk Ser. Mat.*, 34 (1970) 299–321.
[15] M. R. Khan and I. E. Shparlinski, 'On the maximal difference between an element and its inverse modulo n', *Period. Math. Hung.*, **47** (2003), 111–117.
[16] Z. Kh. Rakhmonov, 'On the distribution of values of Dirichlet characters and their applications', *Proc. Steklov Inst. Math.* 207 (1995) 263–272.
[17] I. E. Shparlinski, 'Primitive points on a modular hyperbola', *Bull. Polish Acad. Sci. Math.*, **54** (2006), 193–200.
[18] I. E. Shparlinski, 'Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average', *Michigan Math. J.*, (to appear).
[19] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995.

Department of Mathematics, University of Toronto, Toronto, Ontario M5S 2E4, Canada
E-mail address: frdlndr@math.toronto.edu

Department of Mathematics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden
E-mail address: kurlberg@math.kth.se

Department of Computing, Macquarie University, North Ryde, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au